Amendments to the Specification:

Replace paragraph **[004]** with the following paragraph:

[004] It is well known that a user determines a meaningful password, in the form of, for example, the name of their dog, the birth date of their child or an election year of the favorite candidate. This type of password is easily compromised with investigation. Conversely, a computer can randomly ~~associates~~ associate a password with a user, but this type of password is meaningless to the user and as such difficult to memorize. Consequently, the former method, which is simple, is insecure and the latter method, which is more secure, is difficult to use and often leads to a user writing their password next to their computer, thereby making the system insecure.

Replace paragraph **[005]** with the following paragraph:

[005] The multiplicity of protected system encountered in the daily life of an individual renders the use of a password particularly inconvenient, because a user has to remember a password for each accessible system. For example, the user must remember passwords for accessing network, database, E-mail, bank machine, personal voice mails at home and at work, etc. The plurality of the systems wherein a password is needed favors a single simple password for all systems. In addition, a skilled person may find a predetermined password given sufficient time, rendering the system insecure. In more sophisticated theft situations, "Trojan horse" type viruses can be used to capture a user ID number and password that have been entered at a keyboard or across a network connection. That is, the user thinks he is logging on as usual, but the dialogue box in which the data is entered is really a look-alike window that is capturing his keystrokes.

Please replace paragraph **[006]** with the following paragraph:

[006] To secure access to a network, a further system was developed that relies on a user's personal information. A user requesting access to the network is prompted to answer a series of questions regarding his private life displayed on a computer screen. Such questions might be related to a relative's date of birth, a bone that was broken during childhood, a year of his first car accident, insurance company, address in January 1994, name of his first girlfriend, etc. The computer checks the validity of the answers before allowing access to the user. A

computer is programmed with pertinent questions to ask a user and answers associated therewith, and when the system is initialised, the user enters the answers a first time, they are stored in a memory of the system, and are associated with the user identity. The time taken to answer all the questions prior to gaining access to the system is burdensome. It is evident that a major ~~inconvenient~~ inconvenience with such a system is that a skilled person can find enough information of a personal nature relating to a user for answering properly the questions, and as such render the security ineffectual.

Please replace paragraph **[008]** with the following paragraph:

[008] It is another object of this invention to provide a method for generating a dynamic password.

Please replace paragraph **[0012]** with the following paragraph:

[0012] Advantageously, the invention provides a method of verifying a dynamic password comprising the steps of:

receiving a password comprising a string of characters wherein the characters are sequenced according to a predetermined sequence of variable parameters and static parameters;

identifying static parameters within the string of characters;

determining dynamic parameter values related to the dynamic parameters in accordance with the predetermined sequence;

comparing static parameters received within the string of characters with previously stored static parameters and the received dynamic parameter within the determined dynamic parameters to determine a first comparison result;

wherein upon ~~both~~ the first comparison result being indicative of a match, the dynamic password is validated.

Further advantageously, the invention provides a method of generating a dynamic password comprising the steps of:

providing a process for transforming at least a variable parameter into an ordered string of characters, wherein the process sometimes results in different ordered strings of characters for a same variable parameter; and,

providing at least a variable parameter as a password, the provided variable parameter provided by an individual via a data entry device.

Please replace paragraph **[0016]** with the following paragraph:

[0016] Fig. 2 is a flow diagram of a method of evaluating a dynamic password generated according to the present invention; and

Please replace paragraph **[0017]** with the following paragraph:

[0017] Fig. 3 is an illustration of a computer screen displaying some possible images incorporated in the password~~;~~.

Please replace paragraph **[0018]** with the following paragraph:

[0018] In many large companies, the computer system is organized as a network to reduce the cost of purchasing and installing software on all the stations existing in the company. A main advantage of using a network is to facilitate data accessibility to each employee. However, it is necessary to limit access of a company's network to the company's employees. As such, Fig.1 is an example of a screen display prompting an employee to enter a login identity and an associated password to allow the employee to access the network. An example of a filled dialog box is shown in Fig. 1a. Classically, the login identity is the user's first name, illustrated here, as "Smith" and an exemplary password is "Fido", their dog's name. For security ~~purpose~~ purposes, each character of the password is replaced with a star on the display so that nobody can read it. Each time a user is prompted to enter his password, the password is always identical to the one previously entered by the user unless the user has modified their password during a previous session. An ill-intentioned person can easily find out this type of static password and freely enter a company's network system.

Please replace paragraph **[0019]** with the following paragraph:

[0019] Optionally, to make the system more difficult to break, the network system is organized in such a way that regularly all the employees are prompted to enter a new password. Often, the system allows the users to combine a non-determined number of letters, either small or capital, and digits in their passwords. However, due to the multiplicity of the

systems and the recurrence of the demand, employees often use the same password to which a number is just added. For example, the "Fido" password becomes after a change request "Fidol". During the time period lasting between two successive modifications of a password, the password remains unchanged. A competent person may rapidly find out the password of a user and access a company's network.~~.~~

Please replace paragraph **[0039]** with the following paragraph:

[0039] In the example shown here, only one variable, one static, and one image parameter form part of the predetermined equation for generating the password but of course, there is no limitation as to the number of these parameters. The limit that may be taken into consideration is the good will of the user as to his capacity to memorize parameters to enter when ~~prompt~~ prompted to do so. Additionally, there is no prerequisite to incorporate operations in the equation for generating a dynamic password. Similarly, there is no prerequisite not to incorporate operations while elaborating or programming the dynamic password generating equation for securing a network access.

Please replace paragraph **[0050]** with the following paragraph:

[0050] Numerous other embodiments might be envisioned without departing from the scope and the spirit of the present invention. For example, the description of the invention implicitly inferred that the dynamic password generating equation was identical for all the employees of a company. The difference between the dynamic passwords of two employees ~~login~~ logging in at the same time ~~being~~ can be the static parameters. However, each employee can have a specific dynamic password generating equation. The multiplicity of equations, i.e. as many equations as employees, might be advantageous if an employee leaves the company. In such a case, the equation is deleted and nobody else in the company is affected, otherwise, the whole system must adapt to the departure for keeping the system as secure as possible.